RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ
INDUSTRIELLE

d'invention

Certificat d'utilité

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 28 OCT. 2011

Pour le Directeur général de l'Institut
national de la propriété industrielle
La Directrice des brevets

Martine PLANCHE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITE

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

DATE DE REMISE DES PIÈCES: N° D'ENREGISTREMENT NATIONAL: DÉPARTEMENT DE DÉPÔT: DATE DE DÉPÔT:	Gérard POULIN BREVALEX 3 rue du Docteur Lancereaux 75008 PARIS France
Vos références pour ce dossier: SP 24283 HM 03-024	

1 NATURE DE LA DEMANDE			
Demande de brevet			
2 TITRE DE L'INVENTION			
	PROCEDE D'APPARIEMENT D'UN NOMBRE N DE TERMINAUX RECEPTEURS AVEC UN NOMBRE M DE CARTES DE CONTROLE D'ACCES CONDITIONNEL		
3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE	Pays ou organisation	Date	N°
4-1 DEMANDEUR			
Nom	VIACCESS		
Rue	Les Collines de l'Arche Tour Opéra C		
Code postal et ville	92057 PARIS LA DEFENSE CEDEX		
Pays	France		
Nationalité	France		
Forme juridique	Société anonyme		
5A MANDATAIRE			
Nom	POULIN		
Prénom	Gérard		
Qualité	CPI: 99 0200, Pas de pouvoir		
Cabinet ou Société	BREVALEX		
Rue	3 rue du Docteur Lancereaux		
Code postal et ville	75008 PARIS		
N° de téléphone	0153 83 94 00		
N° de télécopie	01 45 63 83 33		
Courrier électronique	brevets.patents@brevalex.com		
6 DOCUMENTS ET FICHIERS JOINTS	Fichier électronique	Pages	Détails
Texte du brevet	textebrevet.pdf	41	D 28, R 12, AB 1
Dessins	dessins.pdf	3	page 3, figures 7, Abrégé: page 3, Fig.7
Désignation d'inventeurs			

7 MODE DE PAIEMENT				
Mode de paiement	Prélèvement du compte courant			
Numéro du compte client	714			
8 RAPPORT DE RECHERCHE				
Etablissement immédiat				
9 REDEVANCES JOINTES	Devise	Taux	Quantité	Montant à payer
062 Dépôt	EURO	0.00	1.00	0.00
063 Rapport de recherche (R.R.)	EURO	320.00	1.00	320.00
068 Revendication à partir de la 11ème	EURO	15.00	29.00	435.00
Total à acquitter	EURO			755.00

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par
Signataire: FR, Brevalex, G. Poulin
Emetteur du certificat: DE, D-Trust GmbH, D-Trust for EPO 2.0
Fonction
Mandataire agréé (Mandataire 1)

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITE

Réception électronique d'une soumission

Il est certifié par la présente qu'une demande de brevet (ou de certificat d'utilité) a été reçue par le biais du dépôt électronique sécurisé de l'INPI. Après réception, un numéro d'enregistrement et une date de réception ont été attribués automatiquement.

Demande de brevet : X
Demande de CU :

DATE DE RECEPTION	20 février 2004	
TYPE DE DEPOT	INPI (PARIS) - Dépôt électronique	**Dépôt en ligne: X** **Dépôt sur support CD:**
Nº D'ENREGISTREMENT NATIONAL ATTRIBUE PAR L'INPI	0450324	
Vos références pour ce dossier	SP 24283 HM 03-024	

DEMANDEUR

Nom ou dénomination sociale	VIACCESS
Nombre de demandeur(s)	1
Pays	FR

TITRE DE L'INVENTION

PROCEDE D'APPARIEMENT D'UN NOMBRE N DE TERMINAUX RECEPTEURS AVEC UN NOMBRE M DE CARTES DE CONTROLE D'ACCES CONDITIONNEL

DOCUMENTS ENVOYES

package-data.xml	Requetefr.PDF	fee-sheet.xml
Design.PDF	ValidLog.PDF	textebrevet.pdf
FR-office-specific-info.xml	application-body.xml	request.xml
dessins.pdf	indication-bio-deposit.xml	

EFFECTUE PAR

Effectué par:	G. Poulin
Date et heure de réception électronique:	20 février 2004 16:10:00
Empreinte officielle du dépôt	20:0A:BC:1D:2C:FF:26:A3:4F:14:32:80:11:3D:CF:17:8F:5F:BB:F3

/ INPI PARIS, Section Dépôt /

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITE

Désignation de l'inventeur

Vos références pour ce dossier	SP 24283 HM 03-024
N°D'ENREGISTREMENT NATIONAL	
TITRE DE L'INVENTION	
	PROCEDE D'APPARIEMENT D'UN NOMBRE N DE TERMINAUX RECEPTEURS AVEC UN NOMBRE M DE CARTES DE CONTROLE D'ACCES CONDITIONNEL
LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):	
DESIGNE(NT) EN TANT QU'INVENTEUR(S):	
Inventeur 1	
Nom	BEUN
Prénoms	Frédéric
Rue	30, avenue Guy de Maupassant
Code postal et ville	78400 CHATOU - FRANCE
Société d'appartenance	
Inventeur 2	
Nom	BOUDIER
Prénoms	Laurence
Rue	30, avenue Guy de Maupassant
Code postal et ville	78400 CHATOU - FRANCE
Société d'appartenance	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par
Signataire: FR, Brevalex, G. Poulin
Emetteur du certificat: DE, D-Trust GmbH, D-Trust for EPO 2.0
Fonction
Mandataire agréé (Mandataire 1)

PROCEDE D'APPARIEMENT D'UN NOMBRE N DE TERMINAUX RECEPTEURS AVEC UN NOMBRE M DE CARTES DE CONTROLE D'ACCES CONDITIONNEL

DESCRIPTION

DOMAINE TECHNIQUE

L'invention se situe dans le domaine de la sécurisation de données numériques diffusées et des équipements récepteurs destinés à recevoir ces données dans un réseau de distribution de données et/ou services et se rapporte plus spécifiquement à un procédé d'appariement d'un nombre N d'équipements récepteurs de données avec un nombre M de modules externes de sécurité, chaque équipement récepteur étant muni d'un identifiant unique, et chaque module externe de sécurité ayant un identifiant unique.

L'invention concerne également un équipement récepteur susceptible d'être apparié avec une pluralité de modules externes de sécurité pour gérer l'accès à des données numériques distribuées par un opérateur.

ÉTAT DE LA TECHNIQUE ANTÉRIEURE

De plus en plus d'opérateurs offrent des données et services en ligne accessibles au moyen de terminaux munis de processeurs de sécurité. Généralement, les données et services distribués sont embrouillés à l'émission par des clés secrètes et désembrouillés à la réception par les mêmes clés secrètes préalablement mises à la disposition de l'abonné.

Outre les techniques classiques de contrôle d'accès basées sur l'embrouillage à l'émission et le désembrouillage à la réception des données distribuées, les opérateurs proposent des techniques basées sur l'appariement du terminal de réception avec un processeur de sécurité pour éviter que les données et services distribués ne soient accessibles à des utilisateurs munis d'un terminal volé ou d'une carte pirate.

Le document WO 99/57901 décrit un mécanisme d'appariement entre un récepteur et un module de sécurité basé, d'une part, sur le chiffrement et le déchiffrement des informations échangées entre le récepteur et le module de sécurité par une clé unique stockée dans le récepteur et dans le module de sécurité, et d'autre part, sur la présence d'un numéro de récepteur dans le module de sécurité.

Un inconvénient de cette technique provient du fait que l'association entre un récepteur et le module de sécurité qui lui est apparié est établie a priori, et qu'elle ne permet pas à l'opérateur de gérer efficacement son parc d'équipements récepteurs afin d'empêcher le détournement de cet équipement pour des utilisations frauduleuses.

Un but du procédé d'appariement selon l'invention est de permettre à chaque opérateur de limiter les utilisations de son parc de matériel de réception en contrôlant dynamiquement les configurations de l'équipement récepteur et des modules externes de sécurité destinés à coopérer avec cet équipement.

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé d'appariement d'un nombre N d'équipements récepteurs de données avec un nombre M de modules externes de sécurité, chaque équipement récepteur étant muni d'un identifiant unique, et chaque module externe de sécurité ayant un identifiant unique, ce procédé comportant une phase de configuration et une phase de contrôle.

Selon l'invention, la phase de configuration comporte les étapes suivantes :

- mémoriser dans chaque module externe de sécurité une liste d'identifiants d'équipements récepteurs,
- mémoriser dans chaque équipement récepteur une liste d'identifiants de modules externes de sécurité,

et la phase de contrôle consiste à autoriser l'accès aux données si l'identifiant d'un module externe de sécurité connecté à un équipement récepteur est présent dans la liste mémorisée dans cet équipement récepteur, et si l'identifiant dudit équipement récepteur est présent dans la liste mémorisée dans ledit module externe de sécurité, sinon, perturber l'accès auxdites données.

Préférentiellement, la configuration est mise en œuvre uniquement lorsque l'utilisateur connecte un module externe de sécurité à un équipement récepteur.

Dans un mode préféré de réalisation, le procédé selon l'invention comporte une étape dans laquelle l'opérateur transmet à l'équipement récepteur

une signalisation pour gérer la phase de contrôle comportant au moins l'une des consignes suivantes :

- activer la phase de contrôle à une date ou après un délai programmés,
- désactiver la phase de contrôle à une date ou après un délai programmés,
- spécifier une date absolue (respectivement un délai) à partir de laquelle (respectivement au bout duquel) l'activation ou la désactivation de la phase de contrôle est déclenchée,
- annuler ladite date programmée (respectivement ledit délai programmé).

Dans une première variante, l'opérateur transmet en outre à l'équipement récepteur une signalisation comportant un message de suppression de la liste des identifiants mémorisés dans l'équipement récepteur.

Ledit message de signalisation est transmis audit équipement récepteur via un message EMM (Entitlement Management Message, en anglais) spécifique à cet équipement récepteur.

Cette signalisation peut être transmise à un groupe d'équipements récepteurs via un message EMM spécifique audit groupe d'équipements récepteurs.

Dans une deuxième variante, l'opérateur transmet en outre au module externe de sécurité une signalisation comportant un message de suppression de la liste des identifiants mémorisés dans ce module externe de sécurité. Ledit message de signalisation est transmis audit module externe de sécurité via un message EMM spécifique, et peut être transmis à un

groupe de modules externes de sécurité via un message EMM spécifique audit groupe de modules externes de sécurité.

Selon une autre caractéristique du procédé selon l'invention, l'opérateur transmet, d'une part, à un équipement récepteur la liste des M identifiants des modules externes de sécurité via un message EMM spécifique audit équipement récepteur, et d'autre part, à un module externe de sécurité la liste des N identifiants d'équipements récepteurs via un message EMM spécifique audit module externe de sécurité.

Selon une autre variante, l'opérateur transmet, d'une part, à un groupe d'équipements récepteurs la liste des M identifiants de modules externes de sécurité via un message EMM spécifique audit groupe d'équipements récepteurs, et d'autre part, à un groupe de modules externes de sécurité la liste des N identifiants d'équipements récepteurs via un message EMM spécifique audit groupe de modules externes de sécurité.

Dans une autre variante de réalisation, l'opérateur transmet à un groupe d'équipements récepteurs un message de signalisation pour la phase de contrôle dans un flux privé qui est traité par un logiciel dédié exécutable dans chaque équipement récepteur en fonction de l'identifiant dudit équipement récepteur.

Alternativement, la liste d'identifiants de modules externes de sécurité est transmise dans un flux privé à un groupe d'équipements récepteurs et traitée par un logiciel dédié exécutable dans chaque équipement

récepteur en fonction de l'identifiant dudit équipement récepteur, et la liste d'identifiants d'équipements récepteurs est transmise à un groupe de modules externes de sécurité dans un flux privé qui est traité par un logiciel dédié exécutable dans chacun desdits modules externes de sécurité ou dans l'équipement récepteur auquel est connecté un desdits modules externes de sécurité, en fonction de l'identifiant dudit module externe de sécurité.

Dans un exemple d'application du procédé selon l'invention, les données numériques représentent des programmes audiovisuels distribués en clair ou sous forme embrouillée.

Selon une caractéristique supplémentaire, la liste des identifiants des M modules de sécurité mémorisés dans un équipement récepteur est chiffrée, et la liste des identifiants des N équipements récepteurs mémorisés dans un module externe de sécurité est chiffrée.

Avantageusement, le procédé selon l'invention comporte en outre un mécanisme destiné à empêcher l'utilisation d'un EMM transmis à un même module externe de sécurité ou à un même équipement récepteur.

Les messages EMM spécifiques à un module de sécurité ou à un équipement récepteur présentent le format suivant :

```
EMM-U_section() {
table_id = 0x88                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-U_section_length               12 bits
unique_adress_field                40 bits
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

Les messages EMM concernant tous les modules externes de sécurité ou tous les équipements récepteurs présentent le format suivant :

```
EMM-G_section() {
table_id = 0x8A ou 0x8B            8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-G_section_length               12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

Les messages EMM spécifique à un sous-groupe de modules externes de sécurité ou un sous-groupe d'équipements récepteurs présentent le format suivant :

```
EMM-S_section() {
table_id = 0x8E                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-S_section_length               12 bits
shared_address_field               24 bits
reserved                           6 bits
data_format                        1 bit
ADF_scrambling_flag                1 bit
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

Le procédé selon l'invention est mis en œuvre dans un système de contrôle d'accès comportant une pluralité d'équipements récepteurs ayant chacun un identifiant unique et susceptibles de coopérer avec une pluralité de modules externes de sécurité ayant chacun un identifiant unique, chaque module externe de sécurité comportant des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, ce système comportant également une plateforme de gestion commerciale communiquant avec lesdits équipements récepteurs et avec lesdits modules externes de sécurité. Ce système comporte en outre :

- un premier module agencé dans ladite plate-forme de gestion commerciale et destiné à générer des requêtes d'appariement,

- et un deuxième module agencé dans lesdits équipements récepteurs et les modules externes de sécurité et destiné à traiter lesdites requêtes pour préparer une configuration de l'appariement.

Le procédé selon l'invention est utilisable dans une architecture dans laquelle l'équipement récepteur comporte un décodeur et le module externe de sécurité comporte une carte de contrôle d'accès dans laquelle sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur. Dans ce cas, l'appariement est effectué entre ledit décodeur et ladite carte.

Alternativement, le procédé selon l'invention peut être utilisé dans une architecture dans laquelle l'équipement récepteur comporte un décodeur et le module externe de sécurité comporte une interface de sécurité amovible munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur. Dans ce cas, l'appariement est effectué entre ledit décodeur et ladite interface de sécurité amovible.

Le procédé selon l'invention peut également être utilisé dans une architecture dans laquelle l'équipement récepteur comporte un décodeur muni d'une interface de sécurité amovible ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel. Dans ce cas,

l'appariement est réalisé entre ladite interface de sécurité amovible et lesdites cartes de contrôle d'accès.

L'invention concerne également un équipement récepteur susceptible d'être apparié avec une pluralité de modules externes de sécurité pour gérer l'accès à des données numériques distribuées par un opérateur. Cet équipement récepteur comporte :

- une mémoire non volatile destinée à mémoriser une liste de modules externes de sécurité.
- des moyens pour vérifier si l'identifiant d'un module externe de sécurité connecté audit équipement est présent dans la liste mémorisée dans ladite mémoire non volatile.

Dans un premier mode de réalisation, cet équipement récepteur comporte un décodeur et le module externe de sécurité est une carte de contrôle d'accès comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, l'appariement étant dans ce cas effectué entre ledit décodeur et ladite carte.

Dans un deuxième mode de réalisation, cet équipement récepteur comporte un décodeur et le module externe de sécurité est une interface de sécurité amovible munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès auxdites données numériques, l'appariement étant dans ce cas effectué entre ledit décodeur et ladite interface de sécurité amovible.

Dans un troisième mode de réalisation, cet équipement récepteur comporte un décodeur muni d'une interface de sécurité amovible ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel et l'appariement est réalisé entre ladite interface de sécurité amovible et lesdites cartes de contrôle d'accès.

L'invention concerne également un décodeur susceptible de coopérer avec une pluralité de modules externes de sécurité pour gérer l'accès à des programmes audiovisuels distribués par un opérateur, chaque module externe de sécurité ayant un identifiant unique et comportant au moins un algorithme de traitement de données. Ce décodeur comporte :

- une mémoire non volatile destinée à mémoriser une liste de modules externes de sécurité,
- des moyens pour vérifier si l'identifiant d'un module externe de sécurité connecté audit décodeur est présent dans la liste mémorisée dans ladite mémoire non volatile.

Dans une première variante, lesdits modules externes de sécurité sont des cartes de contrôle d'accès dans lesquelles sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

Dans une deuxième variante, lesdits modules externes de sécurité sont des interfaces de sécurité amovibles comportant une mémoire non volatile et destinées à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle

d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

L'invention concerne également une interface de sécurité amovible destinée à coopérer, d'une part, avec un équipement récepteur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès à des données numériques distribuées par un opérateur, chaque carte ayant un identifiant unique et comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques.

Cette interface comporte :

- une mémoire non volatile destinée à mémoriser une liste de cartes d'abonnés,
- des moyens pour vérifier si l'identifiant d'une carte associée à ladite interface est présent dans la liste mémorisée dans ladite mémoire non volatile.

Dans un premier exemple de réalisation, l'interface amovible est une carte PCMCIA (pour Personal Computer Memory Card International Association) comportant un logiciel de désembrouillage de données numériques.

Dans un deuxième exemple de réalisation, l'interface amovible est un logiciel exécutable soit dans l'équipement récepteur soit dans une carte de contrôle d'accès.

Le procédé est piloté par un programme d'ordinateur exécutable sur N équipements récepteurs susceptibles d'être appariés avec M modules externes de sécurité ayant chacun un identifiant unique et dans

lesquels sont stockées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, ce programme comporte des instructions pour mémoriser dans chaque module externe de sécurité une liste d'identifiants d'une partie ou de l'ensemble des N équipements récepteurs, et des instructions pour mémoriser dans chaque équipement récepteur une liste d'identifiants d'une partie ou de l'ensemble des M modules externes de sécurité, des instructions pour contrôler l'identifiant d'un module externe de sécurité connecté à un équipement récepteur et l'identifiant dudit équipement récepteur, et des instructions pour interdire l'accès auxdites données si l'identifiant du module externe de sécurité connecté à l'équipement récepteur n'est pas présent dans la liste d'identifiants préalablement mémorisée dans cet équipement récepteur ou si l'identifiant dudit équipement récepteur n'est pas présent dans la liste d'identifiants préalablement mémorisée dans ledit module externe de sécurité.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif en référence aux figures annexées dans lesquelles :

- la figure 1 représente une première architecture système pour la mise en œuvre de l'appariement selon l'invention,

- la figure 2 représente une deuxième architecture système pour la mise en œuvre de l'appariement selon l'invention,

- la figure 3 représente une troisième architecture système pour la mise en œuvre de l'appariement selon l'invention,

- la figure 4 représente la structure des messages EMM_décodeur de configuration et d'utilisation des fonctionnalités d'appariement selon l'invention,

- la figure 5 représente la structure des messages EMM_carte de configuration des fonctionnalités d'appariement selon l'invention,

- la figure 6 est un diagramme fonctionnel représentant schématiquement les états de la fonction d'appariement embarquée dans un équipement récepteur,

- la figure 7 représente un organigramme illustrant un mode particulier de mise en œuvre de l'appariement selon l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

L'invention va maintenant être décrite dans le cadre d'une application dans laquelle un opérateur diffusant des programmes audiovisuels met en œuvre le procédé selon l'invention pour limiter l'utilisation de son parc d'équipements récepteurs à ses propres abonnés.

Le procédé peut être mis en œuvre dans trois architectures distinctes illustrées respectivement par les figures 1, 2 et 3. Les éléments identiques dans ces trois architectures seront désignés par des références identiques.

La gestion de l'appariement est réalisée à partir d'une plateforme commerciale 1 contrôlée par l'opérateur et communiquant avec l'équipement récepteur installé chez l'abonné.

Dans la première architecture, illustrée par la figure 1, l'équipement récepteur comporte un décodeur 2 dans lequel est installé un logiciel de contrôle d'accès 4, et le module externe de sécurité est une carte de contrôle d'accès 6 comportant des informations relatives aux droits d'accès d'un abonné aux programmes audiovisuels diffusés. Dans ce cas, l'appariement est effectué entre le décodeur 2 et la carte 6.

Dans la deuxième architecture illustrée par la figure 2, l'équipement récepteur comporte un décodeur 2, non dédié au contrôle d'accès, et le module externe de sécurité est une interface de sécurité amovible 8 munie d'une mémoire non volatile et dans laquelle est installé le logiciel de contrôle d'accès 4. Cette interface 8 coopère, d'une part, avec ledit décodeur 2, et d'autre part, avec une carte 6 parmi une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès auxdites programmes audiovisuels.

Dans cette architecture, l'appariement est réalisé entre ladite interface de sécurité amovible 8 et ladite carte de contrôle d'accès 6.

Dans la troisième architecture, illustrée par la figure 3, l'équipement récepteur comporte un décodeur 2 dans lequel est installé un logiciel de contrôle d'accès 4 et qui est connecté à une interface de sécurité amovible 8 ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur 2, et d'autre part, avec une carte 6 parmi une pluralité de cartes de contrôle d'accès conditionnel.

Dans ce cas, l'appariement est effectué entre le décodeur 2 et l'interface de sécurité amovible 8.

La configuration et l'utilisation par l'opérateur de l'appariement résultent de commandes émises par la plateforme de gestion commerciale 1 installée chez l'opérateur.

La description qui suit concerne la mise en oeuvre de l'invention dans le cas d'appariement de N décodeurs dédiés 2 avec M cartes 6. Les étapes mises en œuvre s'appliquent aux trois architectures décrites ci-dessus.

A la sortie d'usine des N décodeurs 2, comme après un téléchargement du logiciel de contrôle d'accès 4 dans chaque décodeur 2, tous les traitements de l'appariement sont inactifs. En particulier :

- aucun identifiant de carte n'est mémorisé dans les décodeurs 2,
- le contrôle par les décodeurs 2 des identifiants des cartes 6 n'est pas actif,
- le contrôle par les décodeurs 2 de la présence de leur propre identifiant dans les cartes 6 n'est pas actif.

De même, à la sortie d'usine des M cartes 6, aucun identifiant de décodeur 2 n'est mémorisé dans les cartes 6.

L'appariement peut alors être configuré et utilisé dans les N décodeurs 2 et dans les M cartes 6 par une requête de l'opérateur via la plateforme de gestion 1 qui émet :

- vers les N décodeurs 2 des messages EMM_décodeur dédiés à l'appariement.

- vers les M cartes 6 des messages EMM_carte dédiés à l'appariement. Ces messages EMM_carte sont émis vers les cartes 6 directement ou intégrés dans des messages EMM_décodeurs.

Les messages EMM_décodeurs permettent d'effectuer les tâches suivantes :

- activer dans les N décodeurs 2 la fonction d'appariement. Dans ce cas chaque décodeur vérifie si l'identifiant d'une carte 6 insérée dans le lecteur de carte du décodeur fait partie des identifiants qu'il a mémorisés et que l'identifiant de ce décodeur 2 fait partie des identifiants de décodeurs mémorisés dans cette carte 6. Si ce n'est pas le cas, une perturbation est appliquée dans l'accès aux données.

- désactiver dans les N décodeurs 2 la fonction d'appariement. Dans ce cas, chaque décodeur 2 ne contrôle ni son identifiant ni celui de la carte.

- charger dans les N décodeurs 2 la liste des M identifiants de cartes 6 appariées à ces décodeurs.

- effacer les identifiants de cartes 6 déjà mémorisés dans les N décodeurs 2.

Les messages EMM_carte permettent de :

- charger dans les M cartes 6 la liste des N identifiants de décodeurs 2 appariés à ces cartes.

- effacer les identifiants des décodeurs 2 déjà mémorisés dans les M cartes 6.

ADRESSAGE DES MESSAGES EMM

Les messages EMM permettant la configuration et l'utilisation des fonctionnalités liées à l'appariement selon le procédé de l'invention sont émis dans une voie EMM d'un multiplex numérique tel que défini par le standard MPEG2/Système et les standards DVB/ETSI.

Cette voie peut diffuser des EMM référençant une adresse de carte(s) permettant de les destiner directement :

- à une carte particulière,
- aux cartes d'un groupe particulier,
- à toutes les cartes,

Cette voie peut diffuser également des EMM référençant une adresse de décodeur(s) permettant de les destiner directement :

- à un décodeur particulier,
- à un groupe particulier de décodeurs,
- à tous les décodeurs,

Les messages destinés à une carte particulière ou à un décodeur particulier sont des EMM-U présentant la structure suivante :

```
EMM-U_section() {
table_id = 0x88                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-U_section_length               12 bits
unique_adress_field                40 bits
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

Le paramètre unique_adress_field est l'adresse unique d'une carte dans un EMM-U carte ou l'adresse unique d'un décodeur dans un EMM-U décodeur.

Les messages destinés à des cartes d'un groupe particulier de cartes ou à des décodeurs d'un groupe particulier de décodeurs sont des EMM-S présentant la structure suivante :

```
EMM-S_section() {
table_id = 0x8E                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-S_section_length               12 bits
shared_address_field               24 bits
reserved                           6 bits
data_format                        1 bit
ADF_scrambling_flag                1 bit
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

Le paramètre shared_adress_field est l'adresse du groupe de cartes dans un EMM-S carte ou l'adresse du groupe de décodeurs dans un EMM-S décodeur. Un décodeur d'un groupe ou une carte d'un groupe est concerné(e) par le message si en outre il (elle) est explicitement désigné(e) dans un champ ADF contenu dans EMM_data_byte et pouvant être chiffré selon l'information ADF_scrambling_flag.

Les messages destinés à toutes les cartes ou à tous les décodeurs sont des EMM-G présentant la structure suivante :

```
EMM-G_section() {
table_id = 0x8A ou 0x8B                 8 bits
section_syntax_indicator = 0            1 bit
DVB_reserved                            1 bit
ISO_reserved                            2 bits
EMM-G_section_length                    12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                       8 bits
    }
}
```

CONTENU DES MESSAGES EMM décodeur

La figure 4 illustre schématiquement le contenu des données EMM_data_byte d'un message EMM_décodeur d'appariement. Ce contenu dépend de la fonction à exécuter par un décodeur 2 pour la configuration ou l'utilisation de l'appariement.

Les données EMM_data_byte incluent les paramètres fonctionnels suivants :

- ADF 20 : complément d'adressage d'un décodeur dans un groupe de décodeurs ; ce paramètre est utile en cas d'adressage par groupe sinon il peut être omis ; il peut être chiffré.

- SOID 22 : identification de message d'appariement selon l'invention, parmi d'autres types de message.

- OPID/NID 24 : identification du parc de décodeurs et du signal de l'opérateur.

- TIME 26 : données d'horodatage de l'émission du message ; ce paramètre est utilisé pour éviter le rejeu du message par un même décodeur

- CRYPTO 28 : identification des fonctions de protection cryptographique appliquées aux paramètres FUNCTIONS 32 ; les paramètres FUNCTIONS peuvent être chiffrés et protégés par une redondance cryptographique 30.

- FUNCTIONS 32 : ensemble des paramètres décrivant la configuration et l'utilisation de l'appariement.

- STBID 34 : adresse unique du décodeur concerné par le message. Ce paramètre est présent dans un EMM-U décodeur, sinon il peut être omis.

Les paramètres fonctionnels ci-dessus sont organisés librement dans les données EMM_data_byte d'un message EMM_décodeur. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

CONTENU DES MESSAGES EMM carte

La figure 5 illustre schématiquement le contenu des données EMM_data_byte d'un message EMM_Carte d'appariement. Ce contenu permet d'inscrire, modifier ou effacer une liste des identifiants de terminaux.

Les données EMM_data_byte incluent les paramètres fonctionnels suivants :

- SOID 40 : identification de l'opérateur.

- ADF 42 : complément d'adressage d'une carte dans un groupe de cartes ; ce paramètre est utile

en cas d'adressage par groupe sinon il peut être omis ; il peut être chiffré.

- CRYPTO 44 : identification des fonctions de protection cryptographique appliquées au paramètre LDA 48 et aux autres paramètres 50 ; les paramètres 48 et 50 peuvent être chiffrés et protégés par une redondance cryptographique 46.

- LDA 48 (Liste de décodeurs autorisées) : ce paramètre contient la liste des identifiants de décodeurs avec lesquels la carte peut fonctionner.

Les données EMM_data_byte peuvent en outre contenir d'autres paramètres 50 concernant des fonctions de la carte autres que l'appariement.

Les paramètres présents dans les données EMM_data_byte sont organisés librement dans ces données d'un message EMM carte. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

CONFIGURATION ET UTILISATION DE L'APPARIEMENT

L'ensemble de paramètres FUNCTIONS 32 dans un EMM_décodeur décrit la configuration et l'utilisation de l'appariement selon l'invention. Cet ensemble de paramètres est une combinaison quelconque des paramètres fonctionnels suivants :

- MODE : ce paramètre active, désactive ou réinitialise la solution d'appariement selon l'invention. Après désactivation, le décodeur ne contrôle pas l'identifiant d'une carte insérée mais conserve la liste des identifiants mémorisés. Après réinitialisation, le décodeur ne contrôle pas

l'identifiant d'une carte insérée et n'a plus d'identifiants de cartes mémorisés

- LCA (Liste de cartes autorisées) : ce paramètre charge dans un décodeur la liste des identifiants de cartes avec lesquelles il peut fonctionner

- Perturbation : ce paramètre décrit la perturbation à appliquer par le décodeur dans l'accès aux données en cas de carte non appariée avec le décodeur

- Date/Délai : ce paramètre caractérise la date ou le délai d'activation ou de désactivation de l'appariement

Les paramètres fonctionnels ci-dessus sont organisés librement dans l'ensemble de paramètres FUNCTIONS 32. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

En outre, dans certains types de service tels qu'une forme d'appariement un décodeur avec une carte, un EMM_décodeur peut transporter un ou plusieurs EMM_cartes. Dans ce cas, l'EMM_carte (les EMM_cartes) est (sont) inclus dans l'ensemble de paramètres FUNCTIONS 32 de façon clairement identifiable par le décodeur qui pourra extraire et fournir à la carte insérée le (les) EMM_carte(s). Une implémentation préférée d'inclusion d'EMM_carte dans l'ensemble de paramètres FUNCTIONS 32 d'un EMM_décodeur est l'usage d'une structure T L V particulière contenant le (les) EMM_carte(s) avec toutes les données d'adressage afférentes.

Une autre utilisation d'EMM_carte dans un EMM_décodeur permet de mémoriser dans la carte que cet EMM_décodeur a déjà été traité par le décodeur, afin d'éviter le rejeu sur un autre décodeur et permettant le traitement unique de cet EMM par un seul décodeur ; sémantiquement ces données signifient « Déjà traité » et sont vérifiées par le logiciel de contrôle d'accès 4 du décodeur 2 quand il traite cet EMM. Une réalisation préférée de ce mécanisme d'anti-rejeu est l'inscription de ces données dans un bloc de données FAC (Facilities Data Block en anglais) de la carte.

FONCTIONNEMENT

Le fonctionnement de l'appariement selon l'invention va maintenant être décrit par référence aux figures 6 et 7.

La figure 6 est un diagramme fonctionnel illustrant schématiquement les états de la fonction d'appariement du logiciel de contrôle d'accès 4 embarqué dans un décodeur 2.

La fonction d'appariement est dans l'état inactif 60 quand le logiciel de contrôle d'accès 4 vient d'être installé ou téléchargé 61 ou quand il a reçu de la plateforme de gestion 1 un ordre de désactivation de l'appariement 62 ou de réinitialisation de l'appariement 64. Dans cet état le logiciel de contrôle d'accès 4 accepte de fonctionner avec une carte 6 insérée dans le décodeur 2 sans vérifier son appariement avec cette carte.

Pour effectuer l'activation de l'appariement entre M décodeurs 2 et N cartes 6, l'opérateur active via la plateforme de gestion 1 :

- un traitement 70 pour définir le mode d'appariement (= actif), et le type de perturbation applicable dans l'accès aux données en cas d'échec de l'appariement,
- un traitement 72 pour définir la liste LCA à charger dans ces N décodeurs des identifiants des M cartes autorisées,
- un traitement 74 pour définir la liste LDA à charger dans ces M cartes des identifiants des N décodeurs autorisés

En fonction de ces informations la plateforme de gestion 1 génère et émet (flèche 76) :

- au moins un message EMM_décodeur pour charger dans la mémoire non volatile des N décodeurs 2 la liste LCA des cartes autorisées 6.
- au moins un message EMM_carte pour charger dans la mémoire non volatile des M cartes 6 la liste LDA des décodeurs autorisés
- au moins un message EMM_décodeur pour charger les paramètres de configuration dans la mémoire non volatile des N décodeurs 2.

La fonction d'appariement dans un décodeur 2 passe à l'état actif 78.

Lors d'une activation de la fonction d'appariement dans un décodeur 2 avec chargement de la liste LCA des cartes 6 autorisées et/ou de la liste LDA des décodeurs 2 autorisés, la prise en compte effective par un décodeur 2 des paramètres de configuration peut être différée dans le temps selon le paramètre Date/Délai pour garantir le chargement effectif de la liste LCA des cartes 6 autorisées dans un décodeur 2 et

de la liste LDA des décodeurs 2 autorisés dans une carte 6.

Lors d'une réactivation de la fonction d'appariement dans un décodeur 2, si la liste LCA des cartes 6 autorisées et/ou la liste LDA des décodeurs 2 autorisés ne nécessite pas de modification, les EMM correspondants ne sont ni générés ni émis.

L'opérateur peut désactiver (étape 80) l'appariement dans un décodeur 2, à partir la plateforme de gestion 1 qui génère et émet (flèche 82) un message EMM adressant le ou les décodeurs 2 concernés et contenant un ordre de désactivation sans effacement du contexte d'appariement 62 ou un ordre de RAZ du contexte d'appariement 64.

La fonction d'appariement dans un décodeur 2 passe à l'état inactif 60.

La prise en compte effective par un décodeur 2 de l'ordre de désactivation peut être différée dans le temps selon le paramètre Date/Délai.

Quel que soit l'état inactif 60 ou actif 78 de la fonction d'appariement, elle peut recevoir de la plateforme de gestion 1 une liste de cartes 6 autorisées LCA par EMM décodeur (étape 72) ou une liste de décodeurs 2 autorisés LDA (étape 74).

La prise en compte d'une des M cartes 6 par la fonction d'appariement d'un des N décodeurs 2 est décrite dans l'organigramme de la figure 7.

A l'insertion (étape 100) d'une carte 6 dans le décodeur 2, le logiciel de contrôle d'accès 4 embarqué dans le décodeur teste (étape 102) si la fonction d'appariement est dans l'état actif 78.

Si la fonction d'appariement dans le décodeur est dans l'état inactif 60, le décodeur accepte de fonctionner avec la carte insérée (108).

Si la fonction d'appariement dans le décodeur est dans l'état actif 78, le logiciel de contrôle d'accès :

- lit l'identifiant de la carte insérée et vérifie (étape 104) si cet identifiant est dans la liste des cartes 6 autorisées mémorisées dans le décodeur 2,
- lit dans la carte insérée la liste des décodeurs autorisés et vérifie (étape 106) si l'identifiant du décodeur 2 est présent dans cette liste,

Les tests 104 et 106 peuvent être exécutés dans n'importe quel ordre.

Si les résultats de ces deux tests d'identifiants 104 et 106 sont positifs, le logiciel de contrôle d'accès 4 accepte de fonctionner avec la carte 6 insérée (étape 108). L'accès aux programmes diffusés est alors possible, sous réserve de conformité des autres conditions d'accès attachées à ces programmes.

Si le résultat d'au moins un des tests 104 et 106 n'est pas positif, le logiciel de contrôle d'accès 4 refuse de fonctionner avec la carte 6 insérée et applique (étape 110) la perturbation dans l'accès aux données telle que définie par l'opérateur. Une telle perturbation peut consister à bloquer l'accès aux programmes diffusés. Elle peut être accompagnée de l'affichage sur l'écran du terminal auquel est associé

le décodeur d'un message invitant l'abonné à insérer une autre carte 6 dans le décodeur 2.

Quand la carte 2 est extraite (étape 112) du décodeur 2, le logiciel de contrôle d'accès passe en attente de l'insertion d'une carte (étape 100)

La perturbation appliquée à l'étape 110 dans l'accès aux données en cas de défaut d'appariement peut être de différente nature telle que :

- Arrêt audio et vidéo sur les chaînes cryptées (obtenu par non soumission des ECM à la carte pour calcul des CW) ;

- Arrêt audio et vidéo sur les chaînes en clair et analogiques (obtenu par message au middleware) ;

- Envoi d'un message au middleware du terminal (exemple : message Open TV).

Cette perturbation peut être utilisée également pour provoquer le blocage de décodeurs volés.

Dans le cas décrit dans la figure 2 où le logiciel de contrôle d'accès 4 est exécuté dans l'interface amovible 8 connectée à un décodeur 2, l'automate décrit dans la figure 4 et l'organigramme décrit dans la figure 5 s'appliquent directement au logiciel de contrôle d'accès embarqué 4 dans cette interface amovible 8.

REVENDICATIONS

1. Procédé d'appariement d'un nombre N d'équipements récepteurs (2) de données avec un nombre M de modules externes de sécurité (6, 8), chaque équipement récepteur (2) étant muni d'un identifiant unique, et chaque module externe de sécurité (6, 8) ayant un identifiant unique, procédé caractérisé en ce qu'il comporte une phase de configuration comportant les étapes suivantes :

- mémoriser dans chaque module externe de sécurité (6, 8) une liste d'identifiants d'équipements récepteurs (2),
- mémoriser dans chaque équipement récepteur (2) une liste d'identifiants de modules externes de sécurité (6, 8),

et une phase de contrôle consistant à autoriser l'accès aux données si l'identifiant d'un module externe de sécurité (6, 8) connecté à un équipement récepteur (2) est présent dans la liste mémorisée dans cet équipement récepteur (2), et si l'identifiant dudit équipement récepteur (2) est présent dans la liste mémorisée dans ledit module externe de sécurité (6, 8), sinon, perturber l'accès auxdites données.

2. Procédé selon la revendication 1, caractérisé en ce que la configuration est mise en œuvre uniquement lorsque l'utilisateur connecte un module externe de sécurité (6, 8) à un équipement récepteur (2).

3. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape dans laquelle l'opérateur transmet à l'équipement

récepteur (2), une signalisation pour gérer la phase de contrôle comportant au moins l'une des consignes suivantes :

- activer la phase de contrôle à une date ou après un délai programmés,

- désactiver la phase de contrôle à une date ou après un délai programmés,

- spécifier une date absolue (respectivement un délai) à partir de laquelle (respectivement au bout duquel) l'activation ou la désactivation de la phase de contrôle est déclenchée,

- annuler ladite date programmée (respectivement ledit délai programmé).

4. Procédé selon la revendication 1, caractérisé en ce que l'opérateur transmet en outre à l'équipement récepteur (2) une signalisation comportant un message de suppression de la liste des identifiants mémorisés dans l'équipement récepteur (2).

5. Procédé selon la revendication 1, caractérisé en ce que l'opérateur transmet en outre au module externe de sécurité (6, 8) une signalisation comportant un message de suppression de la liste des identifiants mémorisés dans ce module externe de sécurité (6, 8).

6. Procédé selon la revendication 1, caractérisé en ce que l'opérateur transmet à un équipement récepteur (2) la liste des M identifiants des modules externes de sécurité (6, 8) via un message EMM spécifique audit équipement récepteur (2).

7. Procédé selon la revendication 1, caractérisé en ce que l'opérateur transmet à un module

externe de sécurité (6, 8) la liste des N identifiants d'équipements récepteurs (2) via un message EMM spécifique audit module externe de sécurité (6, 8).

8. Procédé selon la revendication 1, caractérisé en ce que l'opérateur transmet à un groupe d'équipements récepteurs (2) la liste des M identifiants de modules externes de sécurité (6, 8) via un message EMM spécifique audit groupe d'équipements récepteurs (2).

9. Procédé selon la revendication 1, caractérisé en ce que l'opérateur transmet à un groupe de modules externes de sécurité (6, 8) la liste des N identifiants d'équipements récepteurs (2) via un message EMM spécifique audit groupe de modules externes de sécurité (6, 8).

10. Procédé selon les revendications 3 ou 4, caractérisé en ce que l'opérateur fournit à un équipement récepteur (2) ledit message de signalisation via un message EMM spécifique audit équipement récepteur (2).

11. Procédé selon les revendications 3 ou 4, caractérisé en ce que l'opérateur fournit à un groupe d'équipements récepteurs (2) ledit message de signalisation via un message EMM spécifique audit groupe d'équipements récepteurs (2).

12. Procédé selon la revendication 5, caractérisé en ce que l'opérateur fournit à un module externe de sécurité ledit message de signalisation via un message EMM spécifique audit module externe de sécurité (2).

13. Procédé selon la revendication 5, caractérisé en ce que l'opérateur fournit à un groupe de modules externes de sécurité (6, 8) ledit message de signalisation via un message EMM spécifique audit groupe de modules externes de sécurité (6, 8).

14. Procédé selon les revendications 3 ou 4, caractérisé en ce que l'opérateur transmet à un groupe d'équipements récepteurs (2) dans un flux privé un message de signalisation pour la phase de contrôle, ledit flux privé étant traité par un logiciel dédié exécutable dans chaque équipement récepteur (2) en fonction de l'identifiant dudit équipement récepteur (2).

15. Procédé selon la revendication 1, caractérisé en ce que la liste d'identifiants de modules externes de sécurité (6, 8) est transmise dans un flux privé à un groupe d'équipements récepteurs (2) et traitée par un logiciel dédié exécutable dans chaque équipement récepteur (2) en fonction de l'identifiant dudit équipement récepteur (2).

16. Procédé selon la revendication 1, caractérisé en ce que la liste d'identifiants d'équipements récepteurs (2) est transmise à un groupe de modules externes de sécurité (6, 8) dans un flux privé qui est traité par un logiciel dédié exécutable dans chacun desdits modules externes de sécurité (6, 8) ou dans l'équipement récepteur (2) auquel est connecté chacun desdits modules externes de sécurité (6, 8), en fonction de l'identifiant dudit module externe de sécurité (6, 8).

17. Procédé selon la revendication 1, caractérisé en ce que les données numériques sont distribuées en clair ou sous forme embrouillée.

18. Procédé selon la revendication 17, caractérisé en ce que les données numériques représentent des programmes audiovisuels.

19. Procédé selon la revendication 1, caractérisé en ce que la liste des identifiants des M modules de sécurité mémorisés dans un équipement récepteur (2) est chiffrée.

20. Procédé selon la revendication 1, caractérisé en ce que la liste des identifiants des N équipements récepteurs (2) mémorisés dans un module externe de sécurité (6, 8) est chiffrée.

21. Procédé selon l'une des revendications 6 à 13, caractérisé en ce qu'il comporte en outre un mécanisme destiné à empêcher l'utilisation d'un EMM transmis à un même module externe de sécurité (6, 8) ou à un même équipement récepteur (2).

22. Procédé selon les revendications 6, 7, 10 ou 12, caractérisé en ce que ledit EMM présente le format suivant :

```
EMM-U_section() {
table_id = 0x88                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-U_section_length               12 bits
unique_adress_field                40 bits
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

23. Procédé selon les revendications 8, 9, 11 ou 13, caractérisé en ce que ledit message EMM concerne tous les modules externes de sécurité (6, 8) ou tous les équipements récepteurs (2) et présente le format suivant :

```
EMM-G_section() {
table_id = 0x8A ou 0x8B                 8 bits
section_syntax_indicator = 0            1 bit
DVB_reserved                            1 bit
ISO_reserved                            2 bits
EMM-G_section_length                    12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                       8 bits
    }
}
```

24. Procédé selon les revendications 8, 9, 11 ou 13, caractérisé en ce que ledit message EMM est spécifique à un sous-groupe de modules externes de sécurité (6, 8) ou un sous-groupe d'équipements récepteurs (2) et présente le format suivant :

```
EMM-S_section() {
table_id = 0x8E                         8 bits
section_syntax_indicator = 0            1 bit
DVB_reserved                            1 bit
ISO_reserved                            2 bits
EMM-S_section_length                    12 bits
shared_address_field                    24 bits
reserved                                6 bits
data_format                             1 bit
ADF_scrambling_flag                     1 bit
for (i=0; i<N; i++) {
    EMM_data_byte                       8 bits
    }
}
```

25. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur et le module de sécurité externe (6, 8) comporte une carte de contrôle d'accès (6) dans laquelle sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, et en ce que l'appariement est effectué entre ledit décodeur et ladite carte (6).

26. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur et le module externe de sécurité (6, 8) comporte une interface de sécurité amovible (8) munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès (6) conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur, et en ce que l'appariement est effectué entre ledit décodeur et ladite interface de sécurité amovible (8).

27. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur muni d'une interface de sécurité amovible (8) ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès (6) conditionnel et en ce que l'appariement est réalisé entre ladite interface de sécurité amovible (8) lesdites cartes de contrôle d'accès (6).

28. Equipement récepteur susceptible d'être apparié avec une pluralité de modules externes de sécurité (6, 8) pour gérer l'accès à des données numériques distribuées par un opérateur, caractérisé en ce qu'il comporte :

- une mémoire non volatile destinée à mémoriser une liste de modules externes de sécurité (6, 8),

- des moyens pour vérifier si l'identifiant d'un module externe de sécurité (6, 8) connecté audit équipement est présent dans la liste mémorisée dans ladite mémoire non volatile.

29. Equipement selon la revendication 28, caractérisé en ce qu'il comporte un décodeur et en ce que le module externe de sécurité (6, 8) est une carte de contrôle d'accès (6) comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite carte (6).

30. Equipement selon la revendication 28, caractérisé en ce qu'il comporte un décodeur et en ce que le module externe de sécurité (6, 8) est une interface de sécurité amovible (8) munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel, pour gérer l'accès auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite interface de sécurité amovible (8).

31. Equipement selon la revendication 28, caractérisé en ce qu'il comporte un décodeur muni d'une

interface de sécurité amovible (8) ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel et en ce que l'appariement est réalisé entre ladite interface de sécurité amovible (8) et lesdites cartes de contrôle d'accès (6).

32. Décodeur susceptible de coopérer avec une pluralité modules externes de sécurité (6, 8) pour gérer l'accès à des programmes audiovisuels distribués par un opérateur, chaque module externe de sécurité (6, 8) ayant un identifiant unique et comportant au moins un algorithme de traitement de données, décodeur caractérisé en ce qu'il comporte :

- une mémoire non volatile destinée à mémoriser une liste de modules externes de sécurité (6, 8),

- des moyens pour vérifier si l'identifiant d'un module externe de sécurité (6, 8) connecté audit décodeur est présent dans la liste mémorisée dans ladite mémoire non volatile.

33. Décodeur selon la revendication 32, caractérisé en ce que lesdits modules externes de sécurité (6, 8) sont des cartes de contrôle d'accès (6) dans lesquelles sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

34. Décodeur selon la revendication 32, caractérisé en ce que lesdits modules externes de sécurité (6, 8) sont des interfaces de sécurité amovible (8) comportant une mémoire non volatile et

destinés à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

35. Interface de sécurité amovible destinée à coopérer, d'une part, avec un équipement récepteur (2), et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel, pour gérer l'accès à des données numériques distribuées par un opérateur, chaque carte ayant un identifiant unique et comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, interface caractérisée en ce qu'elle comporte :

- une mémoire non volatile destinée à mémoriser une liste de cartes d'abonnés,
- des moyens pour vérifier si l'identifiant d'une carte associée à ladite interface est présent dans la liste mémorisée dans ladite mémoire non volatile.

36. Interface selon la revendication 35 caractérisée en ce qu'elle consiste en une carte PCMCIA comportant un logiciel de désembrouillage de données numériques.

37. Interface selon la revendication 35 caractérisée en ce qu'elle consiste en un logiciel.

38. Système de contrôle d'accès comportant une pluralité d'équipements récepteurs (2) ayant chacun un identifiant unique et susceptibles de coopérer avec une pluralité de modules externes de sécurité (6, 8) ayant chacun un identifiant unique, chaque module externe de sécurité (6, 8) comportant des informations

relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, ledit système comportant également une plateforme de gestion commerciale (1) communiquant avec lesdits équipements récepteurs (2) et avec lesdits modules externes de sécurité (6, 8), caractérisé en ce qu'il comporte en outre :

- un premier module agencé dans ladite plate-forme commerciale (1) et destiné à générer des requêtes d'appariement,

- et un deuxième module agencé dans lesdits équipements récepteurs (2) et dans lesdits modules externes de sécurité (6, 8) et destiné à traiter lesdites requêtes pour préparer une configuration de l'appariement.

39. Programme d'ordinateur exécutable sur N équipements récepteurs (2) susceptibles de coopérer avec M modules de sécurité (6, 8) ayant chacun un identifiant unique et dans lesquels sont stockées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, caractérisé en ce qu'il comporte des instructions pour mémoriser dans chaque module externe de sécurité (6, 8) une liste d'identifiants d'une partie ou de l'ensemble des N équipements récepteurs 2) , et des instructions pour mémoriser dans chaque équipement récepteur (2) une liste d'identifiants d'une partie ou de l'ensemble des M modules de sécurité (6, 8), des instructions pour contrôler l'identifiant d'un module de sécurité connecté à un équipement récepteur (2) et l'identifiant dudit équipement récepteur (2), et des instructions

pour interdire l'accès auxdites données si l'identifiant du module de sécurité (6, 8) connecté à l'équipement récepteur (2) n'est pas présent dans la liste d'identifiants préalablement mémorisée dans cet équipement récepteur 2) ou si l'identifiant dudit équipement récepteur (2) n'est pas présent dans la liste d'identifiants préalablement mémorisée dans ledit module externe de sécurité (6, 8).

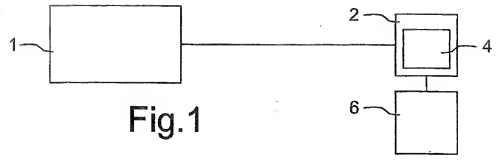

Fig.1

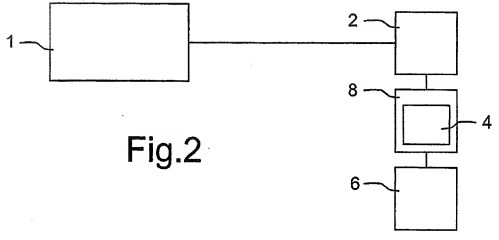

Fig.2

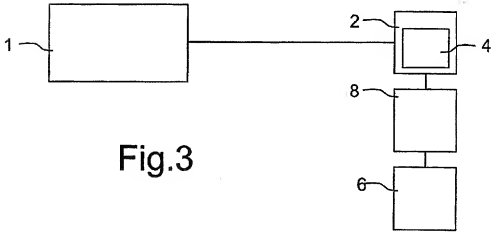

Fig.3

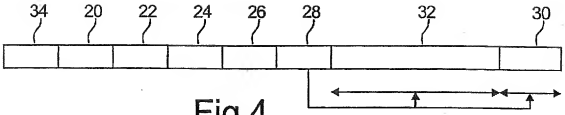

Fig.4

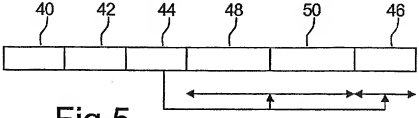

Fig.5

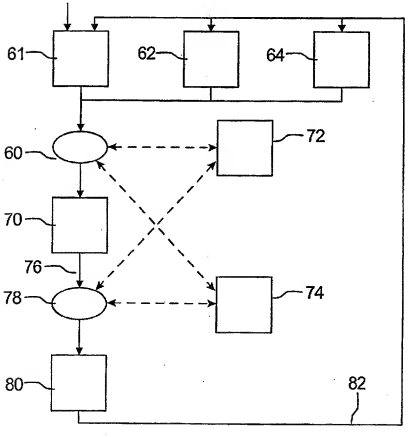

Fig.6

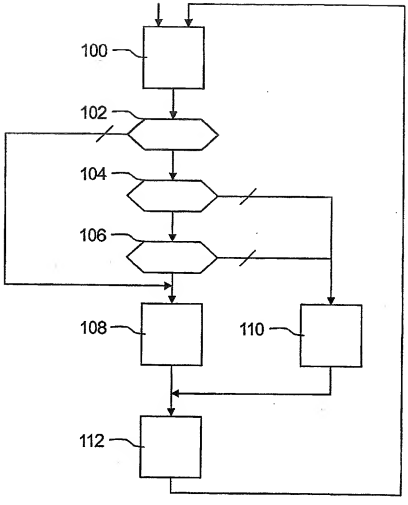

Fig.7